



Beschreibung/Protokoll (Antrag)

Communication/Minutes (Annex)

Notification/Procès-verbal (Annexe)

Datum
Date

20.02.2004

Blatt
Sheet
Feuille

1

Anmelde-Nr.:
Application No.:
Demande n°:

09/327,477

99-204-647.5

MODIFIED 7449

The examination is being carried out on the following application documents:

Text for the Contracting States:

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PL PT RO SE SI
SK TR

Description, pages: 1-40

as originally filed

Claims, No.: 1-23

as originally filed

Drawings, sheets: 1-25

as originally filed

RECEIVED
JUL 14 2004
OFFICE OF PETITIONS

1. The following documents (D) are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

<i>a.m.</i>	D1: ADAMOUSKI F J: 'Encryption technology other than PKI' SECURITY TECHNOLOGY, 1998. PROCEEDINGS., 32ND ANNUAL 1998 INTERNATIONAL CARNAHAN CONFERENCE ON ALEXANDRIA, VA, USA 12-14 OCT. 1998, NEW YORK, NY, USA, IEEE, US, 12 October 1998 (1998-10-12), pages 108-116, XP010309584 ISBN: 0-7803-4535-5
<i>a.m.</i>	D2: MITTRA S: 'IOLUS: A FRAMEWORK FOR SCALABLE SECURE MULTICASTING' COMPUTER COMMUNICATIONS REVIEW, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, US, vol. 27, no. 4, 14 September 1997 (1997-09-14), pages 1-12, XP002931671 ISSN: 0146-4833
<i>a.m.</i>	D3: MENEZES, OORSCHOT, VANSTONE: 'Handbook of applied cryptography' HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, CRC PRESS, 1997, pages 570-572, XP002249713 BOCA RATON, FL, US ISBN: 0-8493-8523-7
<i>a.m.</i>	D4: EP-A-0 715 241 (MITSUBISHI CORP) 5 June 1996 (1996-06-05)

2. The present application does not meet the requirements of Article 52(1) EPC, because the subject-matter of independent claims 1, 17, 20 and 21 does not involve an inventive step in the sense of Article 56 EPC.

- 2.1 Document D1 refers to the management of cryptographic keys. According to the teachings of said document, keying material is made available to users in the form of group keys (corresponding to established groups of users) and individual keys (derived from user-specific information). The group keys are derived from common

EXAMINER: ABDUL HAKIM
A2132

NABAHAR
BEST AVAILABLE COPY

9/2/04